HIPAA Privacy and Security: Training, Compliance, and Metrics Measurement

TMA Privacy Office

Department of Defense

MILITARY MEDICINE TRANSFORMING THE FUTURE

Agenda

Improving HIPAA Implementation

- How do we kick HIPAA up a level?
- What are the levels?
- How do we know we're on track?
- What are some keys to success?

BASIC FACTS OF TRICARE

MISSION

To enhance the Department of Defense and our nation's security by providing health support for the full range of military operations and sustaining the health of all those entrusted to our care

WHAT IS TRICARE

A health care plan using military health care as the main delivery system

- Augmented by a civilian network of providers and facilities
- Serving our uniformed services, their families, retired military, and their families worldwide

9.2 MILLION
TRICARE Eligible Beneficiaries

- 5.0 million TRICARE Prime Enrollees
- 1.62 million TRICARE for Life
- 170,000 TRICARE Plus
- 93,000 US Family Health Plan
- 24,000 TRICARE Reserve Select
- 2.29 million Non-enrolled Users

FACILITIES
MHS Direct Care Facilities

- 70 Military Hospitals
- 411 Medical Clinics
- 417 Dental Clinics

132,500
MHS Personnel

- 88,400 Military
- 44,100 Civilian

18,300
Inpatient Admissions

- 5,300 Direct Care
- 13,000 Purchased Care

1.8 MILLION
Outpatient Visits

- 640,000 Direct Care
- 1.17 million Purchased Care

2200
Births

- 1,000 Direct Care
- 1,200 Purchased Care

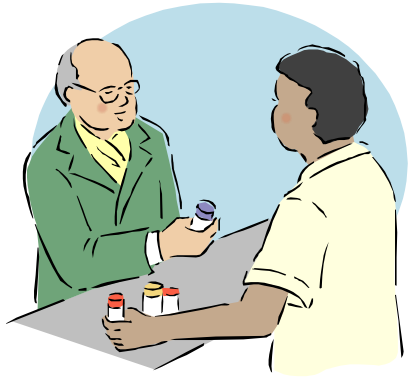
MILITARY MEDICINE TRANSFORMING THE FUTURE

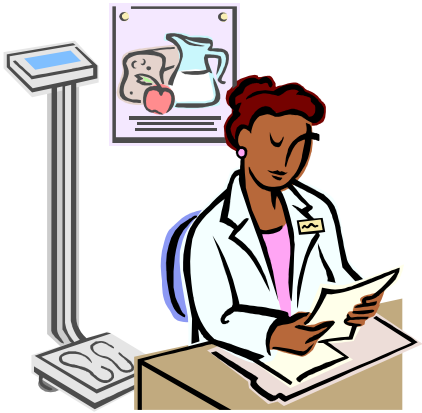
HIPAA Security Metrics

MILITARY MEDICINE TRANSFORMING THE FUTURE

To Keep Up the Good Work...

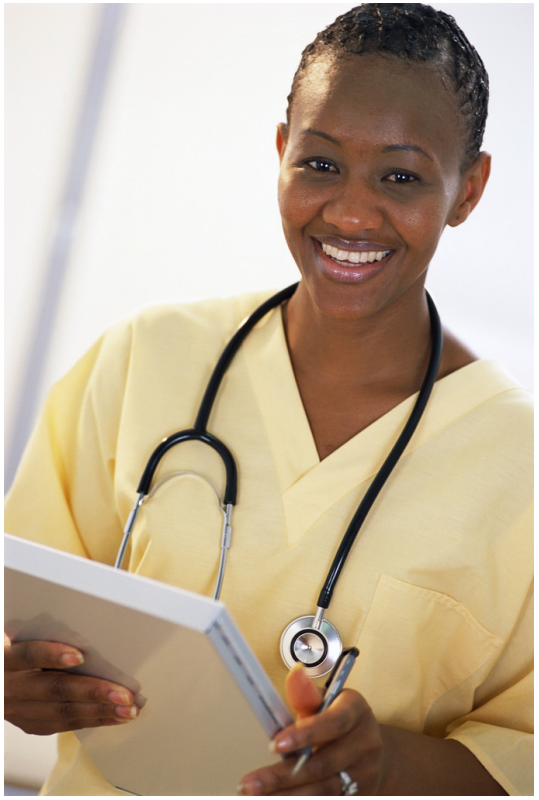
- A lot of things going on in your day-to-day activities
  - Sanctions
  - Complaints and Incidents
  - Access Management
  - Training and Awareness
  - Risk Management
  - Evaluation
  - Workstation Security





...We Have to Sustain and Improve

- To sustain and improve how we implement HIPAA, we must identify for each requirement
  - *Goal*: what we hope to achieve
  - *Objective*: what we specifically seek to do
  - *Implementation Evidence*: proof we do it
  - *Level of Effectiveness*: how well we do it



MILITARY MEDICINE TRANSFORMING THE FUTURE

Key Roles and Requirements

- HIPAA Security Official
- HIPAA Privacy Officer
- Interdisciplinary readiness teams (IRT)
- Senior Executive Staff
- Covered entity workforce
- Self-assessment tool
- Risk analysis / management
- Training and Awareness

MILITARY MEDICINE TRANSFORMING THE FUTURE

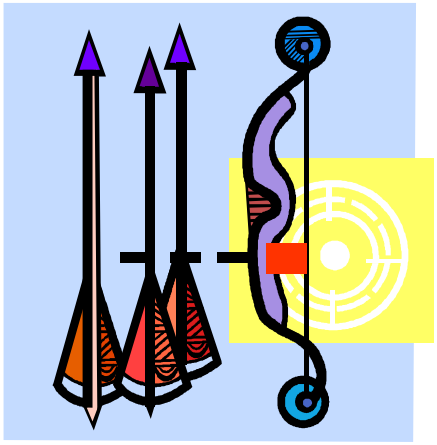
Example: Risk Analysis

- **GOAL**
  - Statement: Technical and organizational policies, procedures, and processes address the potential risks to PHI.
  - Purpose: The target state – where you want to be

MILITARY MEDICINE TRANSFORMING THE FUTURE

Example: Risk Analysis

- **OBJECTIVE**
  - Statement: An IRT assesses and documents risks to PHI on a regular basis and as a result of system, operational, or other changes
  - Purpose: High level approach to aim at the target



MILITARY MEDICINE TRANSFORMING THE FUTURE

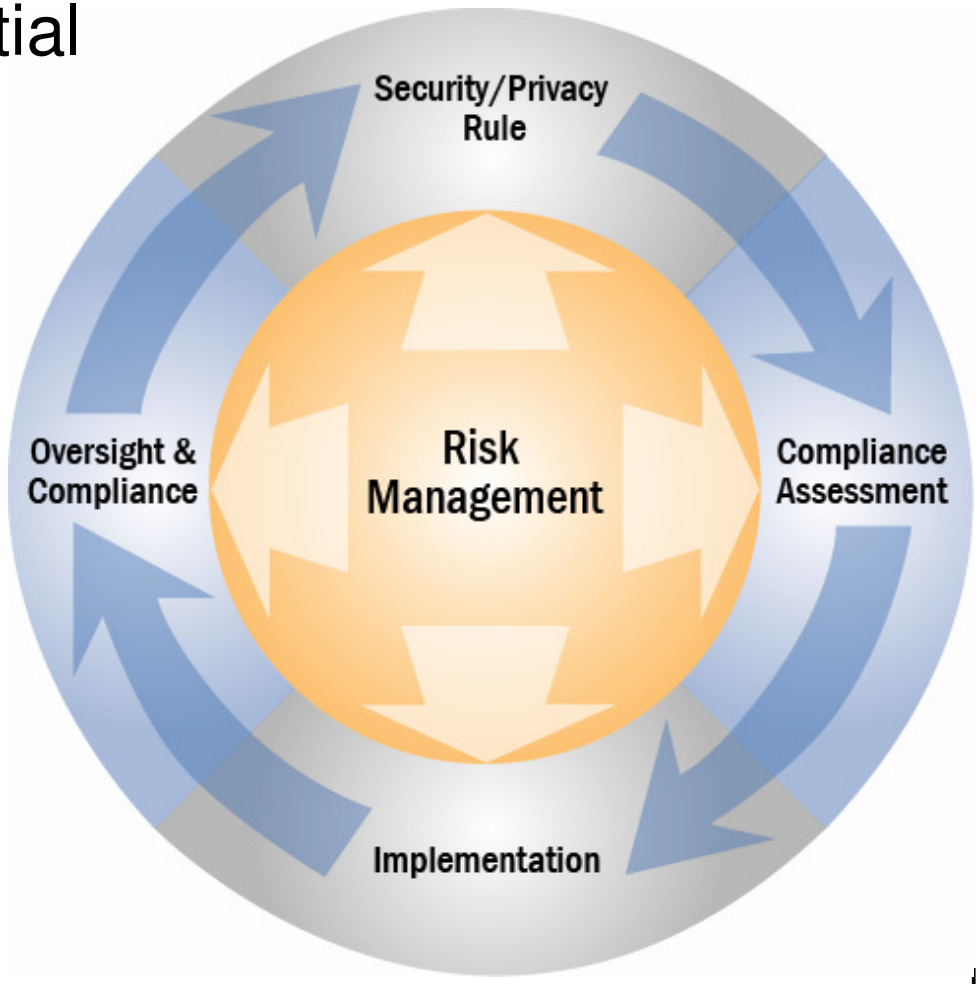
Example: Risk Analysis

- **EVIDENCE OF IMPLEMENTATION**
  - Statement: Has the IRT received senior management approval of the hospital risk assessment conducted in the last 12 months?
  - Purpose: To determine whether basic processes and products are present

MILITARY MEDICINE TRANSFORMING THE FUTURE

Going Forward

- Ongoing cycle of risk management and improvement
- Self-assessment tool: initial compliance assessment
- Prioritized mitigation based on risk analysis
- MHS Metrics Program guides, measures and reports effectiveness of HIPAA implementation
- Institutionalizes activities of risk management



MILITARY MEDICINE TRANSFORMING THE FUTURE

Developing Measures

MILITARY MEDICINE TRANSFORMING THE FUTURE

Development

Federal

Department of Health and Human Services

Office of the Secretary

45 CFR Parts 160, 162, and 164
Health Insurance Reform: Security Standards; Final Rule

(1)(i) *Standard: Security management process.* Implement policies and procedures to prevent, detect, contain, and correct security violations.

(ii) *Implementation specifications:*

(A) *Risk analysis* (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.

- HIPAA Security Regulation analyzed in terms of existing
  - People
  - Processes
  - Tools

MILITARY MEDICINE TRANSFORMING THE FUTURE

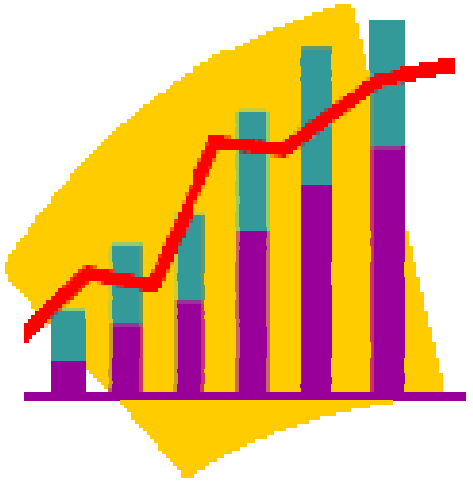
Development

- Adapted metrics approaches from NIST and Federal CIO Council
- Designed metrics that guide as well as measure performance
  - Measures management process as well as compliance products
  - Identifies evidence of compliance that emerges as a natural consequence of doing the work

MILITARY MEDICINE TRANSFORMING THE FUTURE

Two Kinds of Measures

- Management: effectiveness of managing HIPAA implementation
- Statistical: completion percentages



Let's consider a management metric for Risk Analysis

MILITARY MEDICINE TRANSFORMING THE FUTURE

Development: Risk Analysis

- Each metric identifies a Goal, an Approach, and Proof of implementation

Performance Goal	All Covered entity workforce technical and organizational policies, procedures, and processes address the potential risks to PHI.
Performance Objective	The MISRT assesses and documents risks to PHI on a regular basis and as a result of system, operational, or other changes.
Evidence of Implementation	Has the MISRT received senior management approval of the Covered entity workforce risk assessment (risk assessment methodology) conducted in the last 12 months?

MILITARY MEDICINE TRANSFORMING THE FUTURE

Development

- Indicators of Effectiveness support the Evidence of Implementation

■ Objective, obvious actions and products needed to ESTABLISH compliance 	■ What is being done to SUSTAIN and IMPROVE compliance 

MILITARY MEDICINE TRANSFORMING THE FUTURE

Indicators of Effectiveness

- Grouped into five Levels
- Each level represents a more complete and effective state of a requirement
  - Level 1: Policies
  - Level 2: Procedures
  - Level 3: Basic compliance
  - Level 4: Test and validate
  - Level 5: Institutionalize

MILITARY MEDICINE TRANSFORMING THE FUTURE

Level 3: Risk Analysis

- Covered entity workforce has implemented and reinforced procedures for conducting information security risk assessments in a consistent manner through:
  - Distribution to, and periodic acknowledgment from workforce members of their awareness and acceptance of responsibility
  - Management of compliance throughout life of PHI
  - A risk assessment has been scheduled
  - A risk assessment has been conducted

MILITARY MEDICINE TRANSFORMING THE FUTURE

Level 3: Risk Analysis

- Covered entity workforce has implemented and reinforced procedures for conducting information security risk assessments in a consistent manner through:
  - A risk assessment report has been drafted
  - A risk assessment report been presented to senior management
  - Updated position descriptions that accurately identify and reflect skill needs and responsibilities
  - Planning, implementing, and maintaining a training and awareness program

MILITARY MEDICINE TRANSFORMING THE FUTURE

Levels 4 and 5

- Level 4: Policies and procedures are tested and validated for adequacy and effectiveness
- Level 5: Policies, procedures, and practices in the hospital are institutionalized with full senior management support, budgeting, and effective remedial action for prioritized issues

Training/Awareness Level 4 – Example

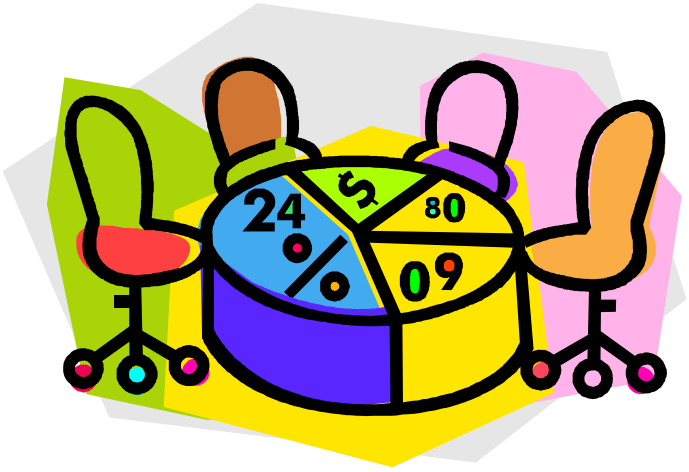
- *THAT* your workforce has completed training is important...
- *WHAT* your workforce does after training is as important

- Do you test and validate that training is working?

MILITARY MEDICINE TRANSFORMING THE FUTURE

Training/Awareness Metrics

- Management and statistical metrics have the same goal, different approach and evidence
- Management metric focuses on processes and products to gauge compliance
- Statistical metric relies on percentage completion of training per job description



MILITARY MEDICINE TRANSFORMING THE FUTURE

Comparing the Two Types of Metrics

- **Goal**: All workforce members understand responsibilities for appropriate use and protection of PHI

Management:

- **Objective**: Develop and implement a local HIPAA awareness and training program for all members of the workforce.

Statistical:

- **Objective**: Train all workforce members on use and protection of PHI.

MILITARY MEDICINE TRANSFORMING THE FUTURE

Evidence of Implementation

- **Management**: Does the HIPAA Security Officer report to senior management monthly on the status of the local training and awareness program?
- **Statistical**: Documented pass percentages for job positions.

Pass Percentage for Job Positions

Summary	
No. of Students:	15720
No. of Students Complete:	13730
No. of Students Incomplete:	1990
Percentage of Students Complete:	87.34%
Students 31-60 Days Delinquent:	133
Students 61-90 Days Delinquent:	163
Students 90+ Days Delinquent:	1057

MHS Illustration

MILITARY MEDICINE TRANSFORMING THE FUTURE

Management and Statistical Metrics

- Handling these separately and keeping them distinct allows for meaningful comparison and trending without bias
- For example
  - A statistical level of effectiveness score of 5, but a management level of effectiveness score of 2 may suggest difficulty in sustaining the Pass Percentages
  - Conversely, a low statistical score and a high management score may indicate positive trends in the near future.

MILITARY MEDICINE TRANSFORMING THE FUTURE

Using a Metric

MILITARY MEDICINE TRANSFORMING THE FUTURE

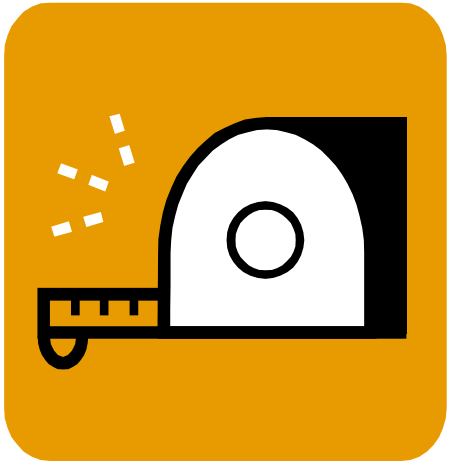
Metrics Provide Multiple Benefits

- **Guide** development and refinement of existing HIPAA program
- **Measure** effectiveness of implementation with enterprise-wide framework
- **Communicate** progress and issues to senior executive staff and higher levels

MILITARY MEDICINE TRANSFORMING THE FUTURE

Guide and Measure Implementation

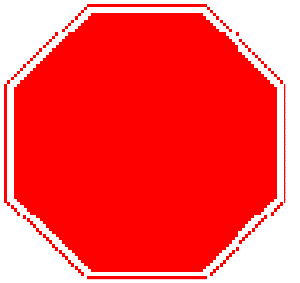
- Initially achieve core compliance but seek to improve over time
- One metric for each HIPAA security requirement
- Suitable for internal and external review

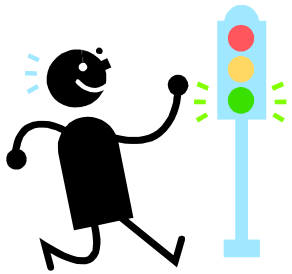


MILITARY MEDICINE TRANSFORMING THE FUTURE

Framework of Effectiveness

- Level 1: Do you have a local policy?
- Level 2: Are your procedures sent to your workforce?





- Level 3: Are local procedures implemented?
- Level 4: Do you test and validate the procedures?
- Level 5: Do senior executive staff fully support the program with funding and resource needs?

MILITARY MEDICINE TRANSFORMING THE FUTURE

Using the Framework of Effectiveness

- Levels of Effectiveness
  - Represent stages of institutional development
  - Requirements for each Level guide steps to take
  - Determining Level: Exhaustive and Cumulative

Level of Effectiveness	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5
	✔	✔	✔		

MILITARY MEDICINE TRANSFORMING THE FUTURE

Responsibilities

- HIPAA Security Official / Privacy Officer
  - Coordinate security activities of the IRT
  - Ensure implementation of requirements
  - Measure effectiveness
  - Report results to senior executive staff

MILITARY MEDICINE TRANSFORMING THE FUTURE

Responsibilities

- IRT manages all related activities
  - Completes self-assessment
  - Conducts risk assessment
  - Executes metrics
  - Brief results to management
- Senior Executive Staff
  - Staffs, funds, and oversees IRT
  - Reviews and authorizes self-assessment reports, risk assessment methodology, metrics
  - Regularly reviews health information protection program

MILITARY MEDICINE TRANSFORMING THE FUTURE

How do you Improve your Program?

- You've measured aspects of your program, and have a lot of information. Now what?

Requirement	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5
Risk Analysis	✔	✔	✔		
Training Management	✔	✔			
Training Statistical	✔	✔	✔	✔	

ILLUSTRATIVE

MILITARY MEDICINE TRANSFORMING THE FUTURE

Improving Your Program

- Enhance your program by through trending, analysis, and information sharing
  - Trending enables you to detect possible problems
  - Analysis determines the details of problems
  - Information sharing promotes awareness to prevent negative impact

MILITARY MEDICINE TRANSFORMING THE FUTURE

Reporting on Effectiveness

- Overdue Requirements
  Reported Monthly
  - *What has not been done*. All requirements that have not been addressed within predetermined threshold (**delinquent**) as determined by risk analysis.

- Active Requirements
  Reported Quarterly
  - *What is being done*. The vulnerabilities whose mitigation is **in progress**. Requirements whose mitigation fall outside of acceptable thresholds are reported as Overdue.

CONCEPTUAL

MILITARY MEDICINE TRANSFORMING THE FUTURE

Reporting on Effectiveness

- Resolved Requirements *Reported Quarterly*
  - *What has been done.* Successfully **addressed** vulnerabilities, as of the current quarter, whose mitigation has been verified and validated.
- Compliant Requirements *Reported Annually*
  - *What does not require action.* The requirements that are **not applicable,** whose risk has been **accepted**, or have been successfully **resolved.**

CONCEPTUAL

MILITARY MEDICINE TRANSFORMING THE FUTURE

Improving the Enterprise

- Reporting effectiveness enables enterprise-wide trending, analysis, and higher level oversight
  - Identify and mitigate local issues efficiently
  - Unify improvements across the enterprise
  - Promote cross-organization collaboration that establishes basis for cost-effective solutions

MILITARY MEDICINE TRANSFORMING THE FUTURE

Keys to Success

- Involvement of HIPAA Security Officials, HIPAA Privacy Officers, and cross-discipline personnel
- Senior leadership buy-in
- Beta testing with diverse site selection
- Receptive to issues, comments, suggestions
- Remember: this is good business

MILITARY MEDICINE TRANSFORMING THE FUTURE

Our Commitment

The TRICARE Management Activity (TMA) Privacy Office is committed to ensuring the Privacy and Security of patient information at every level as we deliver the best medical care possible to those we serve.

TRICARE

TRICARE Management Activity

Confidentiality ----- Integrity ----- Availability

Resources

- TMA Privacy Web Site:
  www.tricare.osd.mil/tmaprivacy/HIPAA.cfm
- Contact us at the TMA Privacy Office:
  privacymail@tma.osd.mil

MILITARY MEDICINE TRANSFORMING THE FUTURE

Backup Slides

MILITARY MEDICINE TRANSFORMING THE FUTURE

Facts and Figures

- TRICARE Management Activity (TMA) is a health care plan using military health as the main delivery system
  - Augmented by a civilian network of providers/facilities
  - Serving our uniformed services, their families, retired military, and their families worldwide
  - 70 Military Hospitals
  - 411 Medical Clinics
  - 417 Dental Clinics
  - 132,500 MHS Personnel

MILITARY MEDICINE TRANSFORMING THE FUTURE

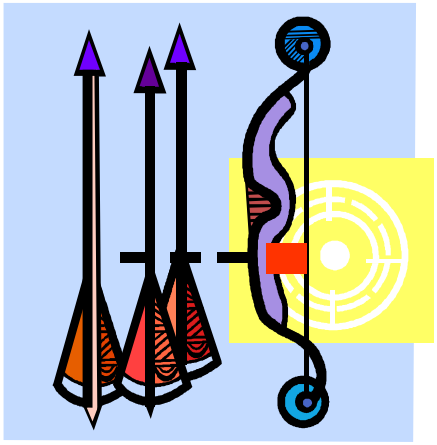
Example: Training and Awareness

- **GOAL**
  - Statement: All Covered entity workforce workforce members understand responsibilities for appropriate protection of ePHI
  - Purpose: The target state – where you want to be

MILITARY MEDICINE TRANSFORMING THE FUTURE

Example: Training and Awareness

- **OBJECTIVE**
  - Statement: Develop and implement a local HIPAA awareness and training program for all members of the workforce
  - Purpose: High level approach to aim at the target



MILITARY MEDICINE TRANSFORMING THE FUTURE

Example: Training and Awareness

- **EVIDENCE OF IMPLEMENTATION**
  - Statement: Does the HIPAA Compliance Officer report to senior management monthly on the status of the local training and awareness program
  - Purpose: To determine whether basic processes and products are present

MILITARY MEDICINE TRANSFORMING THE FUTURE

Indicators of Effectiveness

Establish Compliance

- A risk assessment has been scheduled;
- A risk assessment has been conducted;
- A risk assessment report has been drafted;
- A risk assessment report has been presented to senior management

MILITARY MEDICINE TRANSFORMING THE FUTURE

Indicators of Effectiveness

Sustain and Improve Compliance

- Senior executive staff establishes quality requirements for risk assessment methodology;
- Senior executive staff reviews, documents, and communicates recommendations for improvement of each completed risk assessment methodology;
- Senior executive staff properly constitutes, the MISRT;
- The MISRT conducts regular risk assessments in response to system, operational, and other changes